IT Security Handbook

Contingency Planning

ITS-HBK- 2810.08-01
Effective Date: 20110506
Expiration Date: 20130506
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

Distribution:

NODIS

Approved

Valarie Burks

Valarie Burks
Deputy Chief Information Officer for
Information Technology Security

May 6, 20

Date

Change History

Version	Date	Change Description
1.0		Initial Draft

Table of Contents

1 Introduction and Background

1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).

1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.

1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy*, *NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.

1.4 - *NPR 2810.1, Security of Information Technology,* designates this handbook as a guide of NASA's Contingency Planning (CP) information security controls.

1.5 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.

1.6 - The Contingency Planning control family relates to the preparation of information security response, recovery, and continuity activities to avoid disruptions to critical business processes. Successful contingency planning increases the likelihood that essential information and information systems will be available and assists an organization with maintaining continuity of operations in emergency situations. Effective contingency planning, training, testing, and execution are essential to mitigating the impacts resulting from system and service disruptions.

1.1 - **Applicable Documents**

- *NPD 2810.1, NASA Information Security Policy*
- *NPR 1040.1, NASA Continuity of Operations Planning (COOP) Procedures and Guidelines*
- *NPR 2810.1, Security of Information Technology*
- *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
- *ITS-HBK 2810-08.02, Contingency Planning Guidance and Templates for Plan Development, Maintenance, and Test*
- *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
- *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
- *NIST SP 800-34, Contingency Planning Guide for Information Technology Systems*
- *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
- *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*

2 Contingency Plan (CP-2)

2.1 - **Roles and Responsibilities**

2.1.1 *The Authorizing Official (AO) shall*:

2.1.1.1 - Review and approve proposed contingency plans as a part of the security authorization package.

2.1.2 *The Information System Owner (ISO) shall*:

2.1.2.1 - Develop and maintain a contingency plan for all information systems, as a part of the System Security Plan (SSP), which includes the following:

2.1.2.1.1 Maintaining mission essential and business functions and associated contingency requirements;

2.1.2.1.2 Recovery objectives, restoration priorities, and metrics;

2.1.2.1.3 Contingency roles, responsibilities, assigned individuals with contact information and activities associated with restoring the system;

2.1.2.1.4 Essential mission and business functions despite the information system disruption, compromise, or failure; and

2.1.2.1.5 A business impact assessment (BIA), for information systems under their purview in accordance with *ITS-HBK-2810-08-02*, *NIST SP 800-34*, and *NPR 1040.1*.

2.1.2.2 Coordinate contingency planning activities with the Security Operations Center (SOC).

2.1.2.3 Ensure copies of the approved contingency plan are distributed in a manner consistent with organizationally defined values.

3 Contingency Training (CP-3)

3.1 **Roles and Responsibilities**

3.1.1 *The ISO shall*:

3.1.1.1 Ensure that all personnel involved in information system contingency planning efforts are identified and trained in the procedures and logistics of information system contingency planning and implementation, in compliance with *ITS-HBK 2810-08.02* and *NIST SP 800-34*.

3.1.1.2 Provide refresher training focusing on any changes implemented to the contingency plan.

3.1.1.3 Maintain contingency planning training records.

3.1.1.4 Document refresher training completion in the NASA Security Assessment and Authorization Repository (NSAAR).

4 Contingency Plan Testing and Exercises (CP-4)

4.1 **Roles and Responsibilities**

4.1.1 *The ISO shall*:

4.1.1.1 Conduct controlled tests and/or exercises to gauge the effectiveness of the contingency plans and training and to identify and correct weaknesses and gauge the effectiveness of contingency plans.

4.1.1.2 Execution of contingency plan testing shall follow the schedule laid out in Table 1.

4.1.1.2.1 The Test type identified shall represent the minimum level of testing at the defined interval, but may be exceeded at the discretion of the system owner

4.1.1.3 Review the results of the contingency plan test/exercise, initiate corrective action, and updating the contingency plan to reflect changes.

4.1.1.4 Document completion of the annual contingency plan test/exercise in the SSP and the NSAAR tool.

System Category	Year 1 – Test Type	Year 2 – Test Type	Year 3 – Test Type
Low	Classroom Exercises/Tabletop Written Test	Classroom Exercises/Tabletop Written Test	Classroom Exercises/Tabletop Written Test Integrated Test
Moderate	Classroom Exercises/Tabletop Test	Classroom Exercises/Tabletop Test with Scenarios	Functional Exercises/Simulation Exercise Integrated Test
High	Functional Exercises/Simulation Exercise	Functional Exercises/Simulation Exercise	Functional Exercises/Alternate Site Test Integrated Test

Table 1 - Contingency Plan Test Strategy

5 Alternate Storage Site (CP-6)

5.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

6 Alternate Processing Site (CP-7)

6.1 **Roles and Responsibilities**

6.1.1 *The ISO shall*:

6.1.1.1 Establish an alternate processing site, including necessary agreements, to permit resumption of information system essential mission and business functions within the timelines of the system recovery objectives when the primary processing capabilities are unavailable, in a manner consistent with organizationally defined values.

6.1.1.2 Ensure the availability of equipment and supplies to support the resumption of operations within the time period required.

6.1.1.3 Ensure the alternate processing site is separated from the primary processing site so as not to be susceptible to the same hazards.

6.1.1.4 Ensure alternate processing site agreements are developed/established that contain priority-of-service provisions to meet the information system availability requirements.

6.1.1.5 Ensure the alternate processing site has information security measures equivalent to that of the primary site.

6.1.1.6 Ensure the alternate processing site is fully configured so that it is ready to use as an operational site supporting essential mission and business functions.

7 Telecommunications Services (CP-8)

7.1 **Roles and Responsibilities**

7.1.1 *The ISO shall*:

7.1.1.1 Establish primary and alternate telecommunication service agreements that contain priority-of-service provisions in accordance with the information system availability requirements, and in a manner consistent with organizationally defined values.

7.1.1.2 Request priority of services for the primary and alternate telecommunications services provided by a common carrier that are used for national security emergency preparedness.

7.1.1.3 Obtain alternate communications services with consideration for reducing the likelihood of sharing a single point of failure with the primary communication services.

7.1.1.4 Obtain alternate telecommunication services that are geographically separated from the primary service provider so as to not be susceptible to the same hazards.

7.1.1.5 Ensure service providers of primary and alternate telecommunication services have contingency plans.

8 Information System Backup (CP-9)

8.1 **Roles and Responsibilities**

8.1.1 *The ISO shall*:

8.1.1.1 Ensure backup of user level and system level information.

8.1.1.2 Ensure backup of information system documentation, including security related documentation.

8.1.1.3 Ensure the security of system backup information at the storage site.

8.1.1.4 Ensure backup information is tested to verify media reliability and information integrity.

8.1.1.5 Maintain a record of the results from testing of the backup information and NSAAR tool.

8.1.1.6 Ensure backup copies of the operating system and other critical information systems inventory (including hardware, software, and firmware components) are stored in a separate facility or in a fire-rated container that is not collocated with the operational system.

9 Information System Recovery and Reconstitution (CP-10)

9.1 **Roles and Responsibilities**

9.1.1 *The ISO shall*:

9.1.1.1 Ensure after a disruption, compromise, or failure of an information system that the recovery and reconstitution of the information system is to a known state.

9.1.1.2 Ensure transaction-based recovery is implemented for information systems that are transaction-based. (Note: A system that uses a database management system is a transaction-based example.)

9.1.1.3 Ensure compensating security controls are defined and provided, including procedures and/or mechanisms, for the following circumstances that may inhibit recovery to a known state:

9.1.1.3.1 failure of the system backup capability;

9.1.1.3.2 loss and/or corruption of backup files;

9.1.1.3.3 system information integrity has been compromised by unauthorized access or malware; and

9.1.1.3.4 a hardware component failure, (e.g., server or storage device).

9.1.1.4 Ensure the capability to reimage information system components within the recovery time objectives of the system using configuration controlled and integrity protected disk images that represent a secure, operational state for the components.

10 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
CP	01	Contingency Planning Policy and Procedures	*Main*	*[1]*	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
CP	02	Contingency Plan	*Main*	*[1]*	Reference	List of key contingency personnel who receive copies of the contingency plan.	1. Key individuals, identified by the ISO, who are required for the plan implementation, decisions, support, and/or are impacted by the plan, 2. The AO for the system, 3. The CISO for the Center (or Centers) that are be impacted by the contingency plan.	1. Key individuals, identified by the ISO, who are required for the plan implementation, decisions, support, and/or are impacted by the plan, 2. The AO for the system, 3. The CISO for the Center (or Centers) that are be impacted by the contingency plan.	1. Key individuals, identified by the ISO, who are required for the plan implementation, decisions, support, and/or are impacted by the plan, 2. The AO for the system, 3. The CISO for the Center (or Centers) that are be impacted by the contingency plan.
CP	02	Contingency Plan	*Main*	*[2]*	Frequency	Contingency plan review and	1/Year	1/Year	1/Year

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
						update.			
CP	02	Contingency Plan	*Main*	*[3]*	Reference	List of key contingency personnel who receives updates to the contingency plan.	1. Key individuals, identified by the ISO, who are required for the plan implementation, decisions, support, and/or are impacted by the plan, 2. The AO for the system, 3. The CISO for the Center (or Centers) that are be impacted by the contingency plan, and 4. The NASA SOC Operations Manager.	1. Key individuals, identified by the ISO, who are required for the plan implementation, decisions, support, and/or are impacted by the plan, 2. The AO for the system, 3. The CISO for the Center (or Centers) that are be impacted by the contingency plan, and 4. The NASA SOC Operations Manager.	1. Key individuals, identified by the ISO, who are required for the plan implementation, decisions, support, and/or are impacted by the plan, 2. The AO for the system, 3. The CISO for the Center (or Centers) that are be impacted by the contingency plan, and 4. The NASA SOC Operations Manager.
CP	02	Contingency Plan	*E 3*	*[1]*	Time Period	Maximum time to resumption of essential mission and business functions.			4 Hours
CP	03	Contingency Training	*Main*	*[1]*	Frequency	Refresher training for personnel in contingency planning roles.	1/Year	1/Year	1/Year
CP	04	Contingency Plan Testing and Exercises	*Main*	*[1]*	Frequency	Contingency plan tests and/or exercises.	1/Year	1/Year	1/Year

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
CP	04	Contingency Plan Testing and Exercises	*Main*	*[2]*	Reference	List of tests/exercises.	1. Year1: Classroom Exercises/Tabletop Written Test 2. Year 2: Classroom Exercises/Tabletop Written Test 3. Year 3: Classroom Exercises/Tabletop Written Test - Integrated test	1. Year1: Classroom Exercises/Tabletop Written Test 2. Year 2: Classroom Exercises/Tabletop Written Test with Scenarios 3. Year 3: Functional Exercises/Simulation Exercise	1. Year1: Functional Exercises/Simulation Exercise 2. Year 2: Functional Exercises/Simulation Exercise 3. Year 3: Functional Exercises/Alternate Site Test - Integrated test
CP	07	Alternate Processing Site	*Main*	*[1]*	Time Period	Time for failover of essential mission and business functions to alternate processing site.		Recovery time objectives as specified in the BIA (Business Impact Analysis) and contingency plan	Recovery time objectives as specified in the BIA and contingency plan
CP	08	Telecommunications Services	*Main*	*[1]*	Time Period	Time for failover of telecommunications services.		Recovery time objectives as specified in the BIA and contingency plan	Recovery time objectives as specified in the BIA and contingency plan
CP	09	Information System Backup	*Main*	*[1]*	Frequency	Backups of user-level informaiton.	1/Week	1/Day	1/Day
CP	09	Information System Backup	*Main*	*[2]*	Frequency	Backup of system-level information.	1/Week	1/Day	1/Day
CP	09	Information System Backup	*Main*	*[3]*	Frequency	Backup of information system documentation.	1/Week	1/Day	1/Day
CP	09	Information System Backup	*E 1*	*[1]*	Frequency	Testing of backup information to verify media reliability and information integrity.		4/Year	4/Year

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
CP	10	Information System Recovery and Reconstitution	*E 3*	*[1]*	Reference	Circumstances that can inhibit recovery and reconstitution of systems for which there are compensating controls.		1. Failure of the system backup capability. 2. Loss and/or corruption of backup files. 3. System information integrity has been compromised by unauthorized access or malware. 4. A hardware component failure, (e.g. server or storage device).	1. Failure of the system backup capability. 2. Loss and/or corruption of backup files. 3. System information integrity has been compromised by unauthorized access or malware. 4. A hardware component failure, (e.g. server or storage device).
CP	10	Information System Recovery and Reconstitution	*E 4*	*[1]*	Time Period	Time to reimage components from configuration-controlled and integrity-protected disk images.			Recovery time objectives as specified in the BIA and contingency plan